The diligent use of AI systems: a risk worth taking?

Maarten Herbosch*

Who do you sue when a robot loses your money?[1] This question may sound very abstract, but it has become increasingly relevant. Artificial intelligence (AI) systems are being used in every context imaginable. At the same time, consumers and businesses that use AI systems are confronted with legal uncertainty. This article aims to help clarify this ambiguity, by analysing what conditions determine whether the use of AI systems is diligent.

The question of whether the use of an AI system is diligent, is very relevant for both contract and tort law. Many AI applications, such as autonomous vehicles, are capable of causing damage. If proven to be undiligent, the user of such a system may consequently be held liable, as the duty of diligence plays a central role in establishing tort liability. Similarly, the use of AI systems during contract formation is on the rise. AI systems can be used to advise a party, e.g. by drafting the contract or providing analysis of its content, but also to express a party's will to contract. If the resulting contract turns out to be undesirable, the question of whether the system user has acted diligently may impact his right to annul that contract.

Despite the importance of this question, it is not often discussed in depth in the existing legal doctrine surrounding AI systems. Discussions are often centred around the challenging features of AI systems, and the conclusion that a proper regime is desirable. This article aims to offer a more traditional argument to the discussion, by drawing from the evaluation of the diligence of risks in general tort law. While this article refers to the European level where this is relevant, it is unavoidable to focus on national law as well, as the general tort liability regime is still primarily national. In this regard, the emphasis lies on the Belgian regime, although some other legal systems are also included. Throughout this discussion, the focus is on the diligence of the system user.

1. AI systems

1.1. Artificial intelligence

A proper understanding of the concept of 'artificial intelligence' is essential for this analysis. Unfortunately, a uniform definition does not exist.[2] For this article, we will use

* PhD researcher, Centre for Methodology of Law (KU Leuven) and Research Foundation Flanders (FWO), maarten.herbosch@kuleuven.be

[1] Inspired by T. Beardsworth and N. Kumar, 'Who to Sue When a Robot Loses Your Fortune' <*https://www.bloomberg.com/news/articles/2019-05-06/who-to-sue-when-a-robot-loses-your-fortune*> accessed 1 May 2021.

[2] Also see I. Giuffrida, F. Lederer and N. Vermeyst, 'A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law' 68 [2018] Case Western Reserve Law Review 747, 751; R. Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' 3 [2018] University of Bologna Law Review 180, 184; M. Kaulartz and T. Braegelmann, 'Einführung' in M. Kaulartz and T. Braegelmann (eds), *Rechtshandbuch Artificial Intelligence und Machine Learning* (Beck 2020) 2 ff.; S. Merabet, *Vers un droit d'intelligence artificielle* (Dalloz 2020) 58-59; R. Devillé, N. Sergeyssels and C. Middag, 'Basic Concepts of AI for Legal Scholars' in J. De Bruyne and C. Vanleenhove (eds), *Artificial Intelligence and the Law* (Intersentia 2021) 2.

the definition proposed by the European Commission in its 2018 Communication: "*[a]rtificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals*".[3] We prefer this definition over more traditional definitions, which refer to human intelligence,[4] as the working mechanism of AI systems does not necessarily reflect human cognition.[5] We also prefer this definition over a more recent definition by the same European Commission,[6] which was centred around an annexed list of AI system techniques.[7] The latter definition merely shifts the central challenges in defining AI systems, such as technological neutrality, from the definition itself to the annexed techniques.[8]

The added value of a definition that focuses on autonomy, is that it stresses one of the central challenges that AI systems pose. This autonomy is beautifully illustrated by machine learning (ML) AI systems. As the term *machine learning* suggests, these systems educate themselves. This can be achieved through various techniques, such as supervised, non-supervised and reinforcement learning.[9] With each of these methods, the system learns to recognise patterns,[10] which may be statistical.[11] The general mechanism of these techniques can most easily be explained by comparing them with more traditional non-autonomous

---

Also see note 2.1 in the Opinion of the European Economic and Social Committee on Artificial intelligence — The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (2017/C 288/01).

[3] 'Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe' (April 25th 2018) <*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN*> accessed May 16th 2021, point 1. See similarly: the definition used by the OECD: OECD, 'Recommendation of the Council on Artificial Intelligence' <*https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449*> accessed 29 April 2021, I.

[4] J. McCarthy and others, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence' (1955) <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html> accessed 18 November 2020; N.C. van Oostrom-Streep, 'Over de ethiek van de toekomst en achterhaalde concepten' [2017] WPNR no. 7160, 563; M.-C. Scheau, A.-L. Arsene and G. Popescu, 'Artificial Intelligence/Machine Learning Challenges and Evolution' [2018] International Journal of Information Security and Cybercrime 11, 12.

[5] D.M. Katz, 'Quantitative Legal Prediction - Or - How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry' 62 [2013] Emory Law Journal 909, 918; Giuffrida, Lederer and Vermeyst 755; H. Surden, 'Artificial Intelligence and Law: An Overview' 35 [2019] Georgia State University Law Review 1305, 1315. See with some more nuance (on a more fundamental level): Y. LeCun, Y. Bengio and G. Hinton, 'Deep learning' 521 [2015] Nature 436, 441

[6] Art. 3 (1) of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final (hereafter: the Artificial Intelligence Act).

[7] See Annex I to the proposed Artificial Intelligence Act.

[8] For a more general critical reception of the act, also see P. Hacker, 'A legal framework for AI training data - from first principles to the Artificial Intelligence Act' [2021] Law, Innovation and Technology, < *https://doi.org/10.1080/17579961.2021.1977219*> accessed 29 November 2021; M. Vaele and F. Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' [2021] Computer Law Review international 97, nos. 82-84.

[9] See more technically e.g. E. Alpaydin, *Introduction to Machine Learning* (MIT Press 2010) 21 ff.; G. Rebala, A. Ravi and S. Churiwala, *An Introduction to Machine Learning* (Springer 2019) 19 ff. These techniques may also be combined, e.g. to achieve semi-supervised learning (S.J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach* (Prentice Hall 2010) 695; Rebala, Ravi and Churiwala 22).

[10] H. Surden, 'Machine Learning and Law' 89 [2014] Washington Law Review 87, 89; K.D. Ashley, *Artificial intelligence and legal analytics: new tools for law practice in the digital age* (Cambridge University Press 2017) 234; 'Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe' (April 25th 2018) <*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN*> accessed 16 May 2021, point 3.1; P. Boucher, *How artificial intelligence works: Briefing to the European Parliament* (2019) 2; Surden, 'Artificial Intelligence and Law: An Overview' 1311.

[11] Surden, 'Machine Learning and Law' 95.

computer algorithms. In such a traditional (computer) algorithm, the person creating the algorithm defines what the system should do when a specific event occurs. A vending machine may serve as an example.[12] When someone inserts a coin into the system and subsequently presses a button, the system will release a drink. The programmer of the vending machine has identified both the button that should be pressed and the coin that should be inserted, in order for that specific drink to be served. He has thus created a system that is completely determined by its in- and output: if *X,* then *Y* (if *a coin is inserted and a button is pressed*, then *a drink will be ejected*). At first glance, this is no different in the case of machine learning. As a type of software, ML systems adhere to the same general programming rules and languages as other computer systems.[13] The difference is that the rules that are fed to an ML system are not as closely related to the system's in- and output. Instead, the programmer provides the system with rules (in the same form 'if *X*, then *Y*') which help the system *determine* an appropriate output for a given input. The system requires training to be able to derive the best output for a given input. This process often involves some sort of[14] training data.[15]

The result is that these AI systems present a high degree of autonomy.[16] The output they produce, given a certain input, is to a large(r) degree independent from the instructions which were provided by the programmer of the system.

1.2. Properties and challenges

Before we start delving into the legal framework that governs the use of AI systems – and more particularly: the diligence of using AI systems –, it is necessary to examine these systems in more detail. AI systems present several interesting features that are relevant for our subsequent legal analysis.

1.2.1. AI system potential

Firstly, it is useful to note that AI systems are capable of results that are unattainable for humans.[17] On average, many AI systems outperform human beings at tasks that are

[12] This also happens to be a nice example of a smart contract, see e.g. J.G. Allen, 'Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language' 14 [2018] European Review of Contract Law 307, 313.
[13] Python, for example, is a popular programming language to use for machine learning applications. It is also widely applied for other purposes.
[14] For reinforcement learning, this data is not presented to the system externally. The system is trained by running (internal) simulations, that serve as a source of information.
[15] See e.g. for supervised learning: Alpaydin 21; J. Buyers, *Artificial Intelligence: the practical legal issues* (Law Brief Publishing 2018) 11; Rebala, Ravi and Churiwala 19; A.V. Joshi, *Machine Learning and Artificial Intelligence* (Springer 2020) 10.
[16] Also see M. Ebers, 'Liability For Artificial Intelligence And EU Consumer Law' 12 [2021] JIPITEC 204, 206, no. 7. We use the term 'autonomy' in its everyday meaning to refer to the uncertainty that goes hand in hand with these systems, and not in its philosophical sense, on which see e.g. J. Chirstman, 'Liberalism, Autonomy, and Self-Transformation' 27 [2001] Social Theory and Practice 186, 187 e.
[17] R. Calo, 'Symposium: Singularity: AI and the Law' 41 [2018] Seattle University Law Review 1123, 1124; T. Matsuzaki, 'Ethical Issues of Artificial Intelligence in Medicine' 55 [2018] California Western Law Review 255, 255-273; A.J. Kolber, 'Not-So-Smart Blockchain Contracts and Artificial Responsibility' 21 [2018] Stanford Technology Law Review 198, 205; M. Hatfield, 'Professionally Responsible Artificial Intelligence' 51 [2019] Arizona State Law Journal 1057, 1060; W. Samek and K.-R. Müller, 'Towards Explainable Artificial Intelligence' in W. Samek and others (eds), *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning* (Springer International Publishing 2019) 5-6; S. Cattoor, I. Letten and A. Loose, '[Artificial Intelligence] Inventorship of AI made inventions' [2020] IRDI 7, 8; M. Fierens, E. Van Gool and J. De Bruyne,

traditionally performed by humans.[18] Additionally, AI systems are sometimes capable of performing tasks that humans simply cannot do.[19] Furthermore, AI systems often perform these tasks faster and cheaper than humans would be able to.[20]

The resulting potential is also reflected in the proliferation of AI applications. AI systems can be used to help diagnose diseases,[21] to suggest tv shows,[22] find friends,[23] or even launch missiles.[24] Legal AI applications are on the rise as well. AI systems may be used to manage corporations or to form contracts.[25] The system can, for instance, be used as a source of information, e.g. to authenticate a work of art that the system user may subsequently choose to buy.[26] The system might also help determine the creditworthiness of a party,[27] estimate the value of a piece of real estate,[28] offer advice regarding a financial transaction[29] or review documents in the context of an M&A transaction.[30] AI systems can also be used to

---

'De regulering van artificiële intelligentie (deel 1) – Een algemene stand van zaken en een analyse van enkele vraagstukken inzake consumentenbescherming' [2020-21] RW 962, 964.

[18] Calo 1124. See in the same sense: Matsuzaki 255 ff.; Kolber 205; Hatfield 1060.

[19] See e.g. on the identification of personal attributes based on images of a person's face: Y. Wang and M. Kosinski, 'Deep neural networks are more accurate than humans at detecting sexual orientation from facial images' 114 [2018] Journal of personality and social psychology 246, 246-257 (slightly nuanced in J. Leuner, 'A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation From Facial Images' (*arXiv [cs]* 2019) <*https://arxiv.org/abs/1902.10739*> accessed 16 May 2021.

[20] Superior Court of Justice Ontario 22 November 2018 (Cass v. 1410088 Ontario Inc., 2018 ONSC 6959), <*http://canlii.ca/t/hw728*>; H. Surden, 'Computable Contracts' 46 [2012] U.C. Davis Law Review 629, 638; S. Brown, 'Peeking inside the Black Box: A Preliminary Survey of Technology Assisted Review (TAR) and Predictive Coding Algorithms for Ediscovery' 21 [2015] Suffolk Journal of Trial & Appellate Advocacy 221, 226; R. Bonnaffé, 'Nieuwe technologieën en het recht : de impact van artificiële intelligentie op de rechtspraktijk' [2018] TRV 856, 868; W. Naudé and N. Dimitri, 'The race for an artificial general intelligence: implications for public policy' 35 [2020] AI & SOCIETY 367, 367.

[21] F. Jiang and others, 'Artificial intelligence in healthcare: past, present and future' 2 [2017] Stroke and Vascular Neurology 230, 230 ff.; Hatfield 1065; P. Reusch, 'Produkthaftung' in M. Kaulartz and T. Braegelmann (eds), *Rechtshandbuch Artificial Intelligence und Machine Learning* (Beck 2020) 81, no. 29.

[22] As well as other types of products, see Katz 954; E. He, 'Can artificial intelligence make work more human?' 17 [2018] Strategic HR Review, 263; Hatfield 1065.

[23] Hatfield 1065, which refers to S. Mattu and K. Hill, 'Keep Track Of Who Facebook Thinks You Know With This Nifty Tool' (*Gizmodo*) <*https://gizmodo.com/keep-track-of-who-facebook-thinks-you-know-with-this-ni-1819422352*> accessed 15 March 2021.

[24] M.B. McFarland and A.J. Calise, 'Adaptive nonlinear control of agile antiair missiles using neural networks' 8 [2000] IEEE Transactions on Control Systems Technology 749, 749 ff.

[25] See on an AI system as a corporate management tool: Bonnaffé 860-861; A.-G. Kleczewski, 'L'intelligence artificielle au service des administrateurs : une mise à l'épreuve de la collégialité ?' [2020] TRV 511, 511 ff.

[26] For example A. Chen, R. Jesus and M. Villarigues, 'Using Deep Learning Techniques for Authentication of Amadeo de Souza Cardoso Paintings and Drawings' in P. Moura Oliveira, P. Novais and L.P. Reis (eds), *Progress in Artificial Intelligence* (Springer International Publishing 2019) 172-183. See e.g. <*https://art-recognition.com/*> accessed 30 November 2021.

[27] H. Jacquemin and J.-B. Hubin, 'Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle' in A. de Streel and H. Jacquemin (eds), *L'intelligence artificielle et le droit* (Larcier 2017) 101, no. 27. This application of AI systems qualifies as a 'high risk' application, see point 5 (b) of Annex III to the proposed Artificial Intelligence Act.

[28] E.g. <*https://www.houseprice.ai/*> accessed 19 March 2021.

[29] Hatfield 1065.
This is the case with *high-frequency trading*, see C.R. Korsmo, 'High-Frequency Trading: A Regulatory Strategy' 48 [2013] University of Richmond Law Review, 527-528.

[30] See M. Lauritsen, 'Marketing Real Lawyers in the Age of Artificial Intelligence' 34 [2017] GPSOLO, 68; S. Semmler and Z. Rose, 'Artificial Intelligence: Application Today and Implications Tomorrow' 16 [2017] Duke Law & Technology Review, 86; F. Mebius, 'Software Vervangt Stagair' [2020] Advocatenblad, 30. See on the Kira platform that can be used to this end: O. Hansson, 'Product Review: Kira' 47 [2018] Colorado Lawyer, 13-14; T.P. Sapkota and others, 'Artificial Intelligence That Are Beneficial for Law' 17 [2020] US-China Law Review, 218-219.

determine the content of a contract[31] or to draft or negotiate the contract.[32] Going even further, the user can 'delegate' the decision to contract to the AI system.[33]

1.2.2. AI system challenges and properties

It should be clear that there are also some inherent risks to the use of AI systems. To begin with, it cannot be ruled out that the system will produce erroneous output.[34] This is not always due to poor programming, although this is an important source of AI imprecisions. Even the slightest negligence on the part of the programmer may cause the system to produce incorrect output. This is beautifully illustrated by what is known as reward hacking.[35] The programmer's instructions for the optimization process of the system necessarily include some quantification of success. The system can only improve if it has a way to determine whether a certain outcome is better than another one. In the case of reward hacking, a minor error of the programmer causes the system to be able to achieve 'better' results by taking a shortcut. A good example is an autonomous vacuum robot that starts to *eject* the collected dust, just to be able to clean it up again.[36]

While poor programming may thus contribute to inaccurate results,[37] there are various other sources of AI imprecisions. Deficiencies in the data used to train the system are another example.[38] When discussing erroneous output by AI systems, it is always important to keep the following distinction in mind. AI systems are often employed in statistical

---

[31] A. Hiersche, 'Big Data und Algorithmen im Wettbewersbrecht – Ist das Wettbewersbrecht noch "fit for purpose"?' in T. Jaeger (ed), *Europa 4.0: Die EU im Angesicht politischer und technologischer Herausforderungen* (Jan Sramek Verlag 2018) 66. Also see M.S. Gal and N. Elkin-Koren, 'Algorithmic Consumers' 30 [2016] Harvard Journal of Law & Technology (Harvard JOLT), 310-311 (not necessarily AI).

[32] For drafting: K.D. Betts and K.R. Jaep, 'The Dawn of Fully Automated Contract Drafting: Machine Learning Breathes New Life into a Decades-Old Promise' 15 [2017] Duke Law & Technology Review, 217 ff.; J.M. Lipshaw, 'Halting, Intuition, Heuristics, and Action: Alan Turing and the Theoretical Constraints on AI-Lawyering' 5 [2018] Savannah Law Review, 136; G. Sartor, 'Contracts in the Infosphere' in S. Grundmann (ed), *European Contract Law in the Digital Age* (Intersentia 2018) 271. Also see R. Ambrogi, 'Startup Says It's First Robo-Lawyer for Real Estate Investing', (*LawSites* 25 July 2017) <*https://www.lawsitesblog.com/2017/07/startup-says-first-robo-lawyer-real-estate-investing.html*> accessed 19 March 2021). Also see Arteria, <*https://www.arteria.ai/*> accessed 27 March 2021.
For negotiating: see Pactum, <*https://pactum.com/*> accessed 17 March 2021. Also see Arteria, <*https://www.arteria.ai/*> accessed 27 March 2021. Also see consideration AG in the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

[33] K. Werbach and N. Cornell, 'Contracts ex machina' 67 [2017] Duke Law Journal, 322 (being developed); Sartor 272. This happens in the context of high-frequency trading, see Merabet 368-369; R.T. Kreutzer and M. Sirrenberg, *Understanding Artificial Intelligence: Fundamentals, Use Cases and Methods for a Corporate AI Journey* (Springer 2020) 214 (implicit).

[34] N.A. Greenblatt, 'Self-driving cars and the law' 53 [2016] IEEE Spectrum, 48 ff.

[35] See D. Amodei and others, 'Concrete Problems in AI Safety' [2016] arXiv [cs] 1606.06565, 7 ff.; T. Everitt and others, 'Reinforcement Learning with a Corrupted Reward Channel' [2017] arXiv [cs] 1705.08417, 2; Y. Yuan and others, 'A novel multi-step reinforcement learning method for solving reward hacking' [2019] Applied Intelligence 2874, 2874.

[36] Russell and Norvig 37; D. Hadfield-Menell and others, 'Inverse Reward Design' [2017] NIPS, 1.

[37] Also see Boucher 5; B. Jalaian, M. Lee and S. Russell, 'Uncertain Context: Uncertainty Quantification in Machine Learning' 40 [2019] AI Magazine, 40.

[38] See e.g. Jalaian, Lee and Russell 45 (noise). For a striking example, see J. Nicas, 'Google Has Picked an Answer for You—Too Bad It's Often Wrong' (*The Wall Street Journal* 16 November 2017) <*https://www.wsj.com/articles/googles-featured-answers-aim-to-distill-truthbut-often-get-it-wrong-1510847867*> accessed 22 March 2021; Giuffrida, Lederer and Vermeyst 754. For another striking example, see D. Victor, 'Microsoft Created a Twitter Bot to Learn From Users. It Quickly Became a Racist Jerk' (*The New York Times* 24 March 2016) <*https://www.nytimes.com/2016/03/25/technology/microsoft-created-a-twitter-bot-to-learn-from-users-it-quickly-became-a-racist-jerk.html*> accessed 22 March 2021; Giuffrida, Lederer and Vermeyst 754; R. Janal, 'Extra-Contractual Liability for Wrongs Committed by Autonomous Systems' in M. Ebers and S. Navas (eds), *Algorithms and Law* (Cambridge University Press 2020) 193-194.

environments.[39] In such an environment, some system output that is 'good' does not automatically guarantee a good overall result. If the AI system concerned is a chess computer,[40] the fact that the system suggests/makes a good chess move does not guarantee victory at the end of the game. Instead, it guarantees a good *probability* to achieve a good overall result. Consequently, the fact that the desired outcome is not achieved does not in itself equal a malfunction of the system.

While it is impossible to exclude erroneous AI output, one could argue that this also applies to human performance. Some differences remain, however. AI systems are capable of producing erroneous output that is so manifestly wrong that is unlikely that a human being would make the same mistake.[41] In this context, we can refer to situations where facial recognition software is unable to recognise human beings because of their sex or skin colour.[42]

Another distinction between the mistakes made by an AI system and those made by a human being is the fact that AI errors can be quantified more easily. The performance of an AI system can often be readily quantified by testing the system in a large number of trials, using concepts such as the precision and recall of the system.[43] Given that some requirements are met,[44] this may even be done during the use of the AI system in practice. While it is true that the quantified performance of the AI system may (drastically) change over time, e.g. in case reward function hacking occurs, it should be clear that this performance quantification may nevertheless serve as a very useful tool in evaluating the diligence of the use of the AI system.

In summary, the use of AI systems necessarily entails certain risks of wrong outcomes that are inherently more (easily) quantifiable than human mistakes.

Another challenge in the use of AI systems is their unpredictability.[45] This comes as no surprise, given their autonomy. The fact that the system programmer does not need to foresee every 'correct' output for a given input – and include it directly in the programming – is precisely what allows AI systems to exceed human capabilities. If a human programmer would connect all the possible output to some possible input, the system would be limited to the level of skill of that human.

---

[39] Also see M. Hutter, *Universal Artificial Intelligence: Sequential Decisions based on Algorithmic Probability* (Springer 2004) 28 ff.; Russell and Norvig 480 ff. and 802 ff.; Jalaian, Lee and Russell 43 ff.

[40] See e.g. Rebala, Ravi and Churiwala 195 on Google's AlphaZero chess system.

[41] See e.g. A. Nguyen, J. Yosinski and J. Clune, 'Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images' [2015] Conference on Computer Vision and Pattern Recognition, 427 ff.

[42] S. Lohr, 'Facial Recognition Is Accurate, if You're a White Guy' (*The New York Times* 9 February 2018) <*https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html*> accessed 17 March 2021.

[43] These notions are useful for classification-oriented systems, see e.g. Rebala, Ravi and Churiwala 60. The precision of a system for a certain class, is the amount of correctly identified members of that class, divided by the total amount of identified members (i.e. including wrongfully identified members). The recall of a system for a certain class, is the amount of correctly identified members of that class, divided by the total amount of members of that class (i.e. including those that were not identified).

[44] This requires record keeping of the system parameters and output, also see article 12 of the Artificial Intelligence Act.

[45] R. Yu and G. Ali, 'What's Inside the Black Box? AI Challenges for Lawyers and Researchers' 19 [2019] Legal Information Management 2, 5.

In addition to this unpredictability, AI systems are often said to behave like 'black boxes'.[46] This fundamentally relates to the issue that the complexity of AI algorithms causes them to be unintelligible, even to AI specialists.[47] In that case, it is very hard to explain why the system prefers a certain outcome over another. This lack of *explainability* may sometimes prove to be very problematic, as is the case in the healthcare sector,[48] where AI systems are being used to help doctors diagnose patients.[49] As a result, there is increasingly more interest in the development of *explainable* AI systems.[50] Such AI systems aim to be conceptually intelligible.

2. Diligent use of AI systems

2.1. Relevance

Now that we have a better understanding of AI systems and some of their fundamental properties, we can analyse the legal implications of these properties regarding the diligence of an AI system user. We will start, however, by shortly explaining the importance of the diligence of AI system use.

First, a proper understanding of the duties of diligence is essential for AI system users that want to avoid liability in tort. Numerous AI system applications can cause damage to third parties. This is illustrated by various incidents involving (autonomous) systems that have resulted in emotional or (sometimes deadly) physical injuries.[51] Damage caused by autonomous vehicles may serve as an example.[52] Under the general liability regimes, which are mainly determined by the national legislators of the EU Member States, the duty of

[46] Y. Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' 31 [2017] Harvard JOLT 889, 897; Hatfield 1118 fn. 278; Samek and Müller 6; Yu and Ali 5;; Fierens, Van Gool and De Bruyne 963-964; J. Gerards and R. Xenidis, *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law* (2020) 74; A. Solow-Niederman, 'Administering artificial intelligence' 93 [2020] Southern California Law Review, 657; Devillé, Sergeyssels and Middag 10.

[47] Also see C.E.A. Karnow, 'The Opinion of Machines' 19 [2017] Columbia Science and Technology Law Review, 137.

[48] Samek and Müller 6-7; Devillé, Sergeyssels and Middag 10.
See for the use of AI systems by the government: N.A. Smuha, 'Artificiële intelligentie bij de overheid. Opportuniteiten en uitdagingen vanuit ethisch-juridisch perspectief' [2019] VTOM 43, 51.

[49] Also see Samek and Müller 6-7; Devillé, Sergeyssels and Middag 10. Also see European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence' (8 April 2019) <*https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0168&from=en*> accessed 5 May 2021, 3; G. Vanderstichele, 'Artificiële intelligentie ter ondersteuning van menselijke rechtspraak. De sui-generismethode voor het gebruik van legal analytics in de rechtspraak' [2020] NJW, 610.

[50] Also see A. Adadi and M. Berrada, 'Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)' 6 [2018] IEEE Access, 52139; 15; S.J. Körner, 'Nachvollziehbarkeit von KI-basierten Entscheidungen' in M. Kaulartz and T. Braegelmann (eds), *Rechtshandbuch Artificial Intelligence und Machine Learning* (Beck 2020) 44; Vanderstichele 621; Devillé, Sergeyssels and Middag 10.
Necessary ingredients to this end are explainable data, explainable models and *ex post* explainable decisions, see Körner 49.

[51] See e.g. G. Hallevy, *When Robots Kill: Artificial Intelligence Under Criminal Law* (Northeastern University Press 2013) preface XV (although there was probably no AI system involved here, see e.g. L.A. Kirschgens and others, 'Robot hazards: from safety to security' [2019] arXiv [cs.CY] 1806.06681, 3-4); S. Hoffer, '300-Pound Security Robot Runs Over Toddler At California Shopping Center' (*Huffpost* July 13th 2016) <*https://www.huffpost.com/entry/security-robot-toddler_n_57863670e4b03fc3ee4e8f3a*> accessed 7 May 2021.

[52] See e.g. L. Anat, 'AI Strict Liability vis-a-vis AI Monopolization' 22 [2020] Columbia Science and Technology Law Review 90, 91-92; J. De Bruyne, E. Van Gool and T. Gils, 'Tort Law and Damage Caused by AI Systems' in J. De Bruyne and C. Vanleenhove (eds), *Artificial Intelligence and the law* (Intersentia 2020) 359; European Commission, 'White Paper on Artificial Intelligence: a European approach to excellence and trust' (2020) <*https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf*> accessed 18 March 2021, 12.

diligence plays a fundamental role in determining liability.[53] For example, where there is no violation of a specific legal provision, the general Belgian liability rule (art. 1382 old CC) states that a person may only be liable if he has acted negligently, i.e. less diligently than a normally careful person would have acted in similar circumstances (the so-called *bonus pater familias*).[54]

In this context, the development of a European liability regime for (users of) AI systems has often been advocated,[55] and is currently being investigated by the European Commission.[56] Some have even proposed to grant AI systems a form of legal personality.[57] A proper examination of the diligence of AI system use is very relevant to help determine the desirability of such initiatives. Additionally, even if such legal regimes are adopted, the existing national liability regimes will continue to play an important complementary role for conduct that is not covered by this new European framework.[58]

In the execution of contractual agreements, parties are bound by a standard of diligence as well.[59] For this contractual situation, the discussion is very similar to the one in tort law. Furthermore, the *pre-contractual* diligence of a party may impact the validity of the resulting contract. In this regard, the Belgian regime of *dwaling*/*erreur*, which a mistaken contracting party may invoke to invalidate the contract, requires the mistaken party to have

[53] See for French law: articles 1240-1241 French CC; G. Viney and P. Jourdain, *Les conditions de la responsabilité* (LGDJ 2013) 480; P. Le Tourneau, *Droit de la responsabilité et des contrats* (Dalloz 2020) 43.
See similarly for German law (*Verkehrspflichten* or *Verkehrssicherungspflichten*): BGH 2 October 2012, *NJW* 2013, 48; BGH 2 October 2012, *NJW* 2013, 48; BGH 25 February 2014, *NJW* 2014, 2104; BGH 19 July 2018, *NJW* 2018, 2956; G. Wagner and G. Körner, 'Legal Ignorance in German Law: The Decline of a Once Stringent Standard' [2021] ERPL 253, 275, no. 45.
[54] Antwerpen 30 May 2018, *Limburgs Rechtsleven* 2018, 311; L. Cornelis, *Beginselen van het Belgische buitencontractuele aansprakelijkheidsrecht* (Maklu 1989) 34; T. Vansweevelt and B. Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht* (Intersentia 2009) 127; S. Stijns, *Verbintenissenrecht - Boek 1bis* (die Keure / la Charte 2013) 42.
[55] See e.g. J. Turner, *Robot Rules: Regulating Artificial Intelligence* (Springer International Publishing 2019) 90-91; Anat 92; A.D. Selbst, 'Negligence and AI's human users' 100 [2020] Boston University Law Review 1315, 1375; E. Van Gool, J. De Bruyne and M. Fierens, 'De regulering van artificiële intelligentie (deel 2) – Een analyse van buitencontractuele aansprakelijkheid' [2020-21] RW 1003, 1024. See with more hesitation: G. Wagner, 'Robot Liability' in S. Lohsse, R. Schulze and D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Bloomsbury 2019) 51.
[56] See e.g. <*https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence*> accessed 15 April 2021.
[57] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), point 59 sub f; L.B. Solum, 'Legal Personhood for Artificial Intelligences' [1992] North Carolina Law Review, 1231 ff.; Giuffrida, Lederer and Vermeyst 765; Janal 175-176.
This idea has since been abandoned, see e.g. 'Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe' (25 April 2018) <*https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN*> accessed 16 May 2021. Also see European Economic and Social Committee, 'Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (2017/C 288/01) , point 3.33 and the Expert Group on Liability and New Technologies – New Technologies Formation, 'Report on liability for Artificial Intelligence and other emerging technologies' (2019) <*https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608*> accessed 18 March 2021, 37 ff.
[58] Also see De Bruyne, Van Gool and Gils 370.
[59] See for Belgium: e.g. art. 5.72 (1) wetsvoorstel houdende boek 5 'Verbintenissen' van het nieuw Burgerlijk Wetboek (*Parl.St.* Kamer 2020-2021, no. 1806/001); S. Stijns, *Verbintenissenrecht: Boek 1* (die Keure 2015) 153, no. 196; I. Claeys and T. Tanghe, *Algemeen contractenrecht* (Intersentia 2021) 438, no. 577.
They may even be held to a stricter standard in the case the corresponding obligation is a so-called obligation of result, see e.g. Claeys and Tanghe, 439, no. 579.
For French law: Y. Picod, 'Obligations' [2019] Répertoire de droit civil, nos.77-80.

erred 'excusably'[60] – much like the French regime of *erreur*,[61] but unlike the German *Irrtum* regime.[62] This requirement means that a reasonable party should also have erred in the same circumstances.[63] As such, it closely relates to a requirement of diligence. The condition of an 'excusable' mistake is often even said to be based on the duty of diligence from tort law.[64] Resultingly, the diligence of the use of an AI system may be of great contractual relevance as well. If the AI system was, for example, used to authenticate a painting that was subsequently bought, the relevant question is whether the system user was diligent in the way he or she gathered and processed this information. If the system user did not act diligently, he is not entitled to invoke the Belgian or French regime of mistake.

2.2. Direct approach

The diligence of the use of AI systems thus plays a crucial role in the liability of system users and the validity of the contracts that they might conclude. At the same time, there is a lot of unclarity surrounding this question. Existing literature examining the use of AI systems tends to draw far-reaching consequences from the distinct characteristics of those systems. For example, the autonomy of AI systems and the lack of predictability of their output is said to make it uncertain and unforeseeable whether any damage may arise.[65] As a result, the discussed duty of diligence is said not to be (easily) applicable.[66] In this sense, some authors refer to the increasing autonomy of AI systems. As the system user does not control the actions of the AI system, he or she is said not to be responsible.[67] This is, however, based on the implicit assumption that it was legitimate to use the autonomous system in the first place. This presupposes the diligence of that use.

2.3. Analogy with risk creation

We will investigate this question of diligence from a tort law perspective, as this tort law regime applies analogously to contractual liability and the regime of mistake, as detailed

---

[60] Cass. 6 January 1944, *Arr.Cass.* 1944, 66, *Pas*. 1944, I, 133, note R.H.; H. De Page, *Traité élémentaire de droit civil belge, Tome I: Introduction. Théorie générale des droits et des lois. Les personnes - la famille* (Bruylant 1962) 61; K. Swerts and others, 'Toestemming' in J. Roodhooft (ed), *Bestendig Handboek Verbintenissenrecht* (Wolters Kluwer 2019) II.4 61.

[61] For French law: art. 1132 CC; N. Dissaux, 'Contrat: formation' [2017] Répertoire de procédure civile, no. 139.
For Dutch law: A. Van Kemp, 'Vernietiging van een overeenkomst op grond van dwaling, bedrog of misbruik van omstandigheden' [2009] Bedrijfsjuridische berichten, para 3 *in fine* (violation of a duty to investigate); C.H. Sieburgh, *Algemeen overeenkomstenrecht* (Wolters Kluwer 2018) nos. 241-242.

[62] J. Fuchs, 'Anfechtung von Willenserklärungen' in K. Weber (ed), *Creifelds, Rechtswörterbuch* (Beck 2019) no. 1.

[63] Cass. 6 January 1944, *Arr.Cass.* 1944, 66, *Pas*. 1944, I, 133, note R.H.; Gent 9 January 2012, *TBBR* 2014, 174, note A. Maes; A. De Boeck and J. Waelkens, 'Dwaling' in E. Dirix, B. Tilleman and M. Dambre (eds), *Bijzondere overeenkomsten. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer* (Wolters Kluwer 2017) 29.

[64] Antwerpen 12 June 2006, *RW* 2008-09, 279, note B. Van Den Bergh; J. del Corral, *Dwaling* (Larcier 2011) 66 ff.; B. Demarsin, 'Clausules in verband met dwaling' in G.-L. Ballon and others (eds), *Gemeenrechtelijke clausules, vol. I en II* (Intersentia 2013) 422-423; A. Maes, 'De dwaling in rechte: een nieuw paardenmiddel?' 2014 [2014] TBBR 176, 179; De Boeck and Waelkens 31-32; Swerts and others II.4 61-62.
In French law the general duty of diligence is generally accepted to be the basis of this requirement, see G. Marty and P. Raynaud, *Les obligations. Tome 1: Les sources* (Sirey 1988) 151, no. 148; J. Ghestin and Y.-M. Serinet, 'Erreur' [2018] Répertoire de droit civil, no. 355.

[65] J. Tanghe and J. De Bruyne, 'Aansprakelijkheid voor schade veroorzaakt door autonome motorrijtuigen' 80 [2016-17] RW 963, 973; Jacquemin and Hubin 118, no. 43; Turner 90-91; De Bruyne, Van Gool and Gils 372-373, no. 16 (with the appropriate nuance).

[66] Tanghe and De Bruyne 973; Jacquemin and Hubin 118, no. 43; Turner 90-91.

[67] Tanghe and De Bruyne 973; E. Karner, 'Liability for Robotics: Current Rules, Challenges, and the Need for Innovative Concepts' in S. Lohsse, R. Schulze and D. Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (Bloomsbury 2019) 118.

above. Our discussion will help to show that the general duty of diligence can in fact be applied to the use of AI systems.[68] It will also help provide legal certainty regarding the risks that accompany the use of AI systems.

Some applications of AI systems do not require extensive analysis, as they are clearly undiligent. This is the case, for example, when a party uses an AI system with the intent to cause damage,[69] or in clear violation of the user guidelines of the system without taking proper safety measures.[70] The situation is less clear when the user of the AI system does not violate the system guidelines, but rather violates a soft law provision on the use of AI systems. In this regard, it is relevant that there has been a proliferation of ethical guidelines on the use of AI systems,[71] which often stress the need for transparency and (human) oversight.[72] Similarly, the Artificial Intelligence Act that was proposed by the European Commission is of great interest.[73] This act introduces a certificate requirement for so-called 'high-risk' AI systems (art. 44 Artificial Intelligence Act). Such a certificate may prove to be very relevant for the systems we discuss here as well, even though they are not necessarily 'high-risk'. If a 'low-risk' system meets the strict criteria regarding risk management, data (governance) and record keeping (see art. 9 and subsequent Artificial Intelligence Act) that such a certificate requires, then it is clear that a party who relies on such a system acts more diligently than a party who relies on a system that does not meet the same criteria. It should be clear, however, that this cannot be automatically decisive. A system that meets these criteria may still be used in an undiligent way, and similarly, a system that does not meet them may still be used diligently, by including the necessary precautions.

More generally, a violation of the duty of diligence requires that it is foreseeable that the behaviour concerned might result in some damage.[74] If the future damage is certain, then this requirement is clearly met.[75] It is, on the other hand, useful to clarify that the fact that it is uncertain whether some damage will arise, does not automatically mean that this condition cannot be fulfilled.[76]

---

[68] Also see e.g. W. Kowert, 'The Foreseeability of Human - Artificial Intelligence Interactions' 96 [2017] Texas Law Review 181, 203.

[69] Stijns 42. See similarly: Jacquemin and Hubin 117, no. 43; Van Gool, De Bruyne and Fierens 1009, no. 14
See for German law: §826 BGB.

[70] Jacquemin and Hubin 117, no. 43; Van Gool, De Bruyne and Fierens 1009, no. 14.

[71] High-Level Expert Group on AI, 'Ethics guidelines for trustworthy AI' (8 April 2019) <*https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419*> accessed 17 May 2021. Also see points 138 ff. van de European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)).

[72] See pages 18 ff. of the ethics guidelines. Also see OECD, 'Recommendation of the Council on Artificial Intelligence', <*https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449*> accessed 29 April 2021.

[73] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final.

[74] Cass. 12 November 1951, *Arr.Cass.* 1951, 118 (foreseeability); Cass. 5 May 1971, *Arr.Cass.* 1971, 869; H. Bocken and I. Boone, *Inleiding tot het schadevergoedingsrecht. Buitencontractueel aansprakelijkheidsrecht en andere schadevergoedingsstelsels* (die Keure / la Charte 2014) 91; G. Jocqué, 'Recente ontwikkelingen in het aansprakelijkheidsrecht' in I. Samoy and C. Van Schoubroeck (eds), *Trends en evoluties in het aansprakelijkheids- en verzekeringsrecht* (Intersentia 2019) 45.
See in the same sense for German law: BGH 29 November 1983, *NJW* 1984, 801.

[75] H. Vandeberghe, M. Van Quickenborne and P. Hamelink, 'Aansprakelijkheid uit onrechtmatige daad (1964-1978)' [1980] TPR, 1195.

[76] Cass. 13 June 1978, *Arr.Cass.* 1978, 1202; Luik 15 March 1994, *T.Gez.* 1998–99, 151.

The fact that a party risks the existence of some future, uncertain damage, may still constitute a violation of the duty of diligence.[77] This will, however, only be the case if the engaged risk is abnormal or extraordinary.[78] This is rather sensible: it is *always* impossible to exclude *all* types of risk, regardless of the activity concerned.[79] As a result, the view that any party who takes on *any* risk has violated the duty of diligence is rather impractical.

Due to the impossibility to exclude undesirable output by AI systems as discussed above, there is a close relationship between the use of these systems and the engagement of risks. Similarly, the mere fact that the system user knew *ab initio* that the system might cause some damage, does not suffice to conclude that he or she has not acted diligently. This is only the case when the risk taken is abnormal.

2.3.1. Expertise

The question then becomes whether the use of a specific AI system constitutes an *abnormal* risk.[80] An important first observation in this regard is that the expertise of the liable party is increasingly involved in this assessment under tort law.[81] When a lawyer uses an AI system in the process of a due diligence analysis and blindly trusts its output, the question is not whether a 'normally careful person' would have trusted a similar AI tool for legal analysis, but rather whether a normally careful *lawyer* would have. On a general level, this means that the bar will be set lower for layman consumers using AI systems than it is for businesses that may be using the same AI tool.

In the context of the use of AI systems, we should not only focus on the user's 'traditional' expertise – i.e. the experience as a professional lawyer in our above example of the lawyer using an AI tool –, but also on their expertise in using or even programming AI systems. Such an AI expert can be expected to be more aware of the inherent risk of erroneous system output.

Both of these aspects contribute to the system user's awareness of the risks that the use of the AI system may involve in a specific context. Someone's experience as a professional driver or driving service operator should render him more capable of examining potential hazards in traffic and thus of appreciating the suitability of the use of an autonomous vehicle in a given context. Similarly, the user's experience with AI systems as a programmer should

---

[77] See for German law: R. Wilhelmi, '§823 BGB' in H.P. Westermann, B. Grunewald and G. Maier-Reimer (eds), *Erman BGB: Handkommentar* (Otto Schmidt 2020) no. 77.

[78] Gent 3 October 2018, *RABG* 2019, vol. 5, 438, note J. Benoot; Rb. Marche-en-Famenne 11 December 2003, *Iuvis* 2005, 1446; G. Schamps, *La mise en danger : un concept fondateur d'un principe général de responsabilité : analyse de droit comparé* (Bruylant 1998) 821; B. Dubuisson and others, *La responsabilité civile – Chronique de jurisprudence 1996-2007* (Larcier 2009) 355.
See for a broader view in Germany (where the duty of diligence plays a less fundamental role than in Belgian law): BGH 19 December 1989, *NJW* 1990, 1236; C. Förster, 'BGB § 823 Schadensersatzpflicht' in W. Hau and R. Poseck (eds), *Beck'scher Online-Kommentar BGB* (Beck 2020) no. 302

[79] See in the same sense: H. Cousy, *Problemen van produktenaansprakelijkheid: rechtsvergelijkend onderzoek naar Belgisch, Frans, Nederlands, Duits, Amerikaans, Engels en Europees recht* (Bruylant 1978) 288-289, no. 198; Cornelis 245; Schamps 823-824.

[80] Formulated along the lines of a more traditional approach, this question aims to identify the relevant standard of care for the system user, see e.g. Karner 118.

[81] See for some illustrations: Rb. Mechelen 14 March 1988, *Pas.* 1988, III, 79; Rb. Brussel 20 May 2019, *For.ass.* 2019, vol. 195, 104.

render that user more sensitive to the possibility of undesirable system output, such as an imprecise or undesired steering manoeuvre.

2.3.2. External circumstances

A second observation is that the diligence of some conduct is always evaluated in light of the external circumstances.[82] This is important, as some risks are more normal in one context than in another.[83] The circumstances and goals in or with which the AI system is deployed thus greatly impact the (ab)normality of a certain risk. When someone participates in a game of football, that person runs a greater risk of being tackled than a person who is walking down the street.[84] In an AI context, the risk that an autonomous vehicle, whose aim is to transport people or objects at a high velocity, should collide with an object that suddenly appears out of nowhere, may be deemed normal. If, however, we consider an autonomous vacuum cleaning robot, a similar risk of running into people at high velocity should be deemed abnormal.

Some literature approaches this incorporation of the external circumstances from the perspective of the victim.[85] A woman participating in a game of baseball is then said to have accepted the risk that she might be hit in the face by a ball,[86] which would not apply if she had been walking in her garden. This is sometimes captured by the phrase that "*the timorous may stay home*".[87] The result would then be that the victim of the undiligent act cannot claim compensation for any damage, as he or she is said to have 'accepted' the risk of this damage in advance.[88]

This does not fully apply under Belgian law.[89] In Belgian law, 'risk acceptance' is a rather misleading label. It merely describes the inclusion of the external circumstances in the duty

---

[82] Cornelis 36; R. Kruithof and others, 'Verbintenissenrecht: Overzicht van rechtspraak (1981-1992)' [1994] TPR, 336; Vansweevelt and Weyts 128 ff.; Stijns 43 ff.; Bocken and Boone 90-91.
See for German law: BGH 3 February 2004, *NJW* 2004, 1449 (on the necessary precautions); A. Staudinger, 'Kommentar zum § 823' in R. Schulze (ed), *Bürgerliches Gesetzbuch: Handkommentar* (Nomos 2019) no. 65; Förster nos. 309-310; G. Wagner, '§ 823 Schadensersatzpflicht' in M. Habersack (ed), *Münchener Kommentar zum Handelsgesetzbuch: Band 7* (Beck 2020) no. 38.
See for American law: J.A. Joyce and H.C. Joyce, *Treatise on Damages Covering the Entire Law of Damages Both Generally and Specifically* (The Banks Law 1903) §149 L.H. Dietz and others, 'Negligence' in *American Jurisprudence* (Thomson Reuters 2021) §138.
[83] See for example Gent 16 June 2005, *RABG* 2007, vol. 19, 1289, note R. Sierens; Gent 30 March 2006, *RABG* 2007, vol. 19, 1281; R. Sierens, 'Abnormaal agressief voetbalspel: is er risicoaanvaarding door het slachtoffer?' [2007] RABG, 1294; Vansweevelt and Weyts 129.
For French law: Viney and Jourdain 501-502.
For American law: S.M. Speiser, C.F. Krause and A.W. Gans, *American Law of Torts* (Westlaw 2020) §9:43.
[84] See e.g. Bergen 19 October 2015, *T.Verz.* 2017, 334.
[85] See e.g. G. Martyn, R. Devloo and Y. Jorens, *Een kennismaking met recht en rechtspraktijk* (die Keure / la Charte 2018) 290; G. Lindemans, *Schuldeiser & rechtspersoon* (Intersentia 2019) 64; J. Maeschalck, A. Vermeersch and K. De Saedeleer, *Sportrecht* (die Keure / la Charte 2019) 18.
[86] Antwerpen 19 maart 2008, *T.Verz.* 2010, 337.
[87] Court of Appeals of New York 16 April 1929, Murphy v. Steeplechase Amusement Co., 166 N.E., 173; Speiser, Krause and Gans §9:50.
[88] See e.g. Gent 16 October 2014, *NJW* 2016, 37, note T. Verheyen; Rb. Brussel 13 January 2009, *TOO* 2016, vol. 4, 554 (summary); Rb. Oost-Vlaanderen 15 December 2015, *VAV* 2016, vol. 1, 62; Pol. Antwerpen 15 November 2015, *VAV* 2016, vol. 3, 86; Pol. Vilvoorde 18 January 2018, *VAV* 2018, vol. 4, 80; N. Broeckx, *Orgaantransplantatie* (Intersentia 2018) 538 (passingly); Martyn, Devloo and Jorens 290; Lindemans 64; Maeschalck, Vermeersch and De Saedeleer 18.
See for French law: J. Mouly and C. Dudognon, 'Sport – Activités sportives' [2019] Répertoire de droit civil, no. 108.
[89] Belgian law differs a bit from e.g. French law in this respect, as the theory of risk acceptance is more commonly accepted there, despite some criticism. See e.g. Cass.fr. 4 November 2010, no. 09-65947, *Bull.civ.* 2010, II, no. 176 (liability for movable

of diligence.[90] 'Risk acceptance' by the victim is only relevant insofar it constitutes a breach of his proper duty of diligence. In that case, the victim must proportionally bear some of the costs of his damage.[91] Consequently, this requires the risk that was taken by the victim to be 'abnormal' as well.

Regardless of whether 'risk acceptance' is accepted, this does help clarify that the conduct of (potential) victims may have a big impact on the relevant risks that were created by the AI system user. It is unreasonable to require the system user to anticipate all types of possible behaviour. Consequently, it suffices that a diligent party takes the foreseeable, reasonable actions of other parties into account.[92]

2.3.3. Precautionary measures

Before we discuss the impact of precautionary measures, it is useful to clarify that the risk itself consists of several distinct components which should be considered. On the one hand, there is the component of *probability*, i.e. the odds that some damage will occur. On the other hand, there is the resulting damage, i.e. the *expected loss*.[93] This distinction is also beautifully captured by the American *Learned Hand test*.[94] This test offers a very economic perspective to the question of whether it is diligent to take a specific risk.[95] It states that a party has not acted diligently when he or she has neglected to take precautionary measures, on the condition that the cost of those precautionary measures was lower than the expected cost of the damage (Probability × Expected loss > Burden of precaution).

This clarifies that an AI system user does not have to take all imaginable precautionary measures to act diligently. Put differently: even if someone did not take some specific

objects); E. Cordelier, 'Un arbitrage sans concession de la Cour de cassation : l'acceptation des risques en butte à une « exclusion définitive » des terrains de sport ?' [2003] D., nr II ff.; Viney and Jourdain 673 ff. See for the acceptance of the theory: Mouly and Dudognon no. 108 ff.

[90] M. Adams, 'Is risico-aanvaarding een zelfstandig juridisch concept?' [1993-94] RW 304, 305; Vansweevelt and Weyts 171. For French law: Viney and Jourdain 675.

[91] Cass. 17 February 2017, *TBBR* 2021, 101, note S. Somers (implicit); Rb. Luik 16 November 2007, *T.Agr.R.* 2008, 105; Dubuisson and others 358; Vansweevelt and Weyts 167; A. Lenaerts, 'L'influence de la faute intentionnelle du préposé sur le partage de responsabilités entre le commettant et la victime négligente : application par répercussion du principe fraus omnia corrumpit?' [2015] JT 844, 844; S. Somers, 'Het niet-toerekenen van de eigen fout van een naaste bij rechtstreekse schade: reden om het ook niet toe te rekenen bij onrechtstreekse materiële schade?' 2021 [2021] TBBR, 103.
In the American law, this view is currently applied under the doctrine of *comparative fault* (or, more specifically, that of *comparative negligence*) see e.g. Supreme Court of California, Knight v. Jewett, 24 August 1992, 3 *Cal.4th*, 296; Speiser, Krause and Gans §13:1; M.P. Thomas and others, *California Civil Practice Torts* (Westlaw 2020) §1:42; Dietz and others §954.

[92] Also see G.P. Fletcher, 'Fairness and Utility in Tort Theory' [1972] Harvard Law Review, 550; Viney and Jourdain 480; Wagner no. 481. See in the same sense: Gent 19 September 2013, *TBBR* 2015, 212, note S. ILLEGEMS (the court indicated that the operator of a swimming pool should have placed a warning sign next to the hot air vent of a steam cabin. This would clearly not suffice if a negligent visitor would neglect to read the warning sign); Rb. Tongeren 16 October 2006, *RW* 2007–08, 658; S. Illegems, 'De waarschuwingsverplichting van de uitbater van een zwembadcomplex' [2015] TBBR, 218

[93] See (formulated differently): H.L. Feldman, 'Prudence, Benevolence, and Negligence: Virtue Ethics and Tort Law' [2000] Chicago-Kent Law Review, 1442.
For German law: Wagner no. 478.
For American law: Feldman 1442 (implicit).

[94] Circuit Court of Appeals 9 January 1947, United States v. Carroll Towing Co., 159 F.2d, 169. See about this B.A. White, 'Risk-utility analysis and the learned hand formula: hand that helps or hand that hides' [1990] Arizona Law Review, 77 ff.; D.P. O'Gorman, 'Contract Law and the Hand Formula' [2014] Louisiana Law Review, 156. Also see §3 Restatement Third of Torts on liability for physical and emotional harm.

[95] See similarly, on the expectation value of the damage, in Germany: Wagner no. 478.

precautionary measures, he may still have acted diligently.[96] Consequently, the risk-taking party should only be expected to take precautionary measures if they are reasonable.[97]

While this test heavily stresses the economic costs of precautionary measures as a deciding factor, we would argue that they are not the only decisive element.[98] The nature of the potential damage should also be considered, as well as the means of the risk-taking party.[99] Physical injuries caused to persons are, for example, inherently more severe than property damage. Consequently, this also relates to the context in which the AI system was used. The risk taken by a lawyer who does not fully verify the output of a document review AI tool, in order to save time and money, seems inherently more acceptable – and thus less abnormal (although it may still be abnormal depending on the precise context) – than the risk taken by a doctor who does not verify an AI system's evaluation of a patient's brain scan. Similarly, it seems reasonable to set a higher precautionary standard for a wealthy professional business than for an amateur or a consumer.

Furthermore, different precautionary measures can affect different aspects of the risk. First, some measures can affect the probability of damage. In this regard, the use of a less accurate AI system is less diligent than the use of a more accurate system, if the latter is available. This also shows that the user of the system should take reasonable precautions to ensure that the accuracy of the system is as optimal as can reasonably be expected in the specific situation. If the system user is responsible for the training of the AI system, the duty of diligence requires that he ensures that the system has been sufficiently trained before it is applied. There may be an important limitation to the amount of required training, however. At some point, the temporal or financial costs of marginally improving the system may become unreasonably large.

The probability damage may also be minimised beyond the training and accuracy of the system. If the system can be used in a different way, which minimises the probability of damage, with no significant disadvantage to the system user, the system should only be used in this way. In this respect, it is for example less diligent to use an autonomous vehicle in very poor weather conditions.[100]

Second, some precautionary measures can reduce the size of the damage that might occur (i.e. the expected loss). This may be achieved in different ways. If, for example, the AI system can be used in two distinct ways and the first way entails less potential damage than the second, without a significant disadvantage to the system user, then only the first application will be diligent. As is the case for the probability of damage, the system user is

[96] E.g. Luik 15 February 1999, *JT* 1999, 398.
For German law: Förster no. 301 (very broadly).
[97] For German law: BGH 28 June 1965, *NJW* 1965, 1760 (at §839 BGB); BGH 2 October 2012, *NJW* 2013, 48; BGH 25 February 2014, *NJW* 2014, 2104; BGH 19 July 2018, *NJW* 2018, 2956; Förster no. 309; Wagner no. 466; A. Teichmann, 'Kommentar zum § 823' in R. Stürner (ed), *Jauernig BGB: Handkommentar* (Beck 2021) no. 35.
For the American law: Court of Appeals of New York 18 June 1981, Akins v. Glens Falls City School District, 424 *N.E.2d*, 531.
Among other things, this obviously entails that these measures must be *possible*, see e.g. Förster no. 304.
[98] For German law: BGH 29 November 1983, *NJW* 1984, 801; Wagner no. 479.
[99] For German law: BGH 29 November 1983, *NJW* 1984, 801.
[100] Also see Tanghe and De Bruyne 966.

also expected to take reasonable precautions to limit the potential damage. This is often less convenient, which is why case law usually stresses the importance of precautionary measures that limit the probability of damage.[101]

2.3.4. Human behaviour as a reference

On a more general level, the duty of diligence – and the creation of risks in particular – is very much aimed at *human* behaviour. Consequently, the comparison with human behaviour may be very interesting in order to evaluate the performance of AI systems. To assess whether the use of an AI system with a particular accuracy constitutes an abnormal risk, it is relevant to compare the accuracy of a human using the AI system with the accuracy of a human performing the task on its own or with human help. If, for example, data provided by insurance companies allows us to quantify the risk of damage when humans perform a certain task,[102] we can compare this with the quantified average performance of the AI system. As it is generally sufficiently diligent to delegate a task to another human being with sufficient expertise,[103] this may help to show that the similar delegation to an AI system that outperforms the average qualified human, is equally diligent. This means that the availability of qualitative data is not only essential for the training of AI systems, but for their evaluation as well.

Conclusion

In this article, we have examined the diligence of the use of AI systems. These systems will play an increasingly important role in our society, as the number of AI applications is on the rise. As a result, these systems are becoming increasingly relevant from a legal perspective as well. This holds for a variety of legal domains, which include contract law and tort law. Consequently, the question of whether the use of an AI system is diligent is of crucial importance. This question determines whether consumers and businesses that use AI systems, may be held liable for damage that was caused by their system. It may also determine whether a party can invoke the invalidity of an undesirable contract when this contract was closed using an AI system.

We have approached this question of diligent AI system use from a traditional tort law perspective. In general, the use of the system should not violate existing legislation. This may, for example, currently be the case for the use of autonomous vehicles. AI systems should also meet the relevant product requirements, in the instances where particular legislation provides them.

---

[101] See e.g. Antwerpen 2 February 1995, *AJT* 1994–95, 496, note B. Wylleman; Brussel 25 October 2005, *RGAR* 2007, vol. 10, no. 14322; Brussel 12 January 2016, *TBO* 2016, 161; Pol. Gent 19 November 2007, *T.Agr.R.* 2008, 109.
For German law: Wilhelmi no. 89
Analogous in American law (for risk acceptance by the victim): Supreme Court of Delaware 24 July 1991, Furek v. University of Delaware, 594 *A.2d*, 506 ("*one does not assume a risk unless he appreciates its danger but takes no steps to avoid it*"); Court of Appeal of California 1 July 1997, Lowe v. California League of Prof. Baseball, 56 *Cal.App.4th*, 112; Feldman 1439 and 1441.

[102] Schamps 878-879.

[103] See implicitly in the context of seeking (human) advice: J. Stevens, 'Hoe gemeen is het gemene recht?' [1979-80] RW 1602, 1617; A.-S. Baudry and C. De Koker, *Valkuilen bij aankoop van een onroerend goed: Wilsgebreken, verborgen gebreken en verborgen non-conformiteit* (Larcier 2016) 37.

For a more detailed analysis, we have expanded on the analogy between the use of an AI system, for which it is impossible to exclude unforeseen output, and the engagement of risks. This allowed us to apply the existing tort law doctrine on the diligence of risk engagement to the use of AI systems. The engagement of risk and, correspondingly, the use of an AI system is diligent, unless the engaged risk is abnormal. Resultingly, we have focused our attention on the different factors that govern risk (ab)normality.

Our analysis has clarified that the expertise of the AI system user is a very relevant factor. On a general level, the standard of diligence is stricter for an expert or a business than it is for a layman consumer. A professional driver that uses an autonomous vehicle is, for example, expected to be more aware of the potential dangers of using a high-speed vehicle. More specifically, the user's experience with AI systems is also quite relevant, as this should render him more aware of potential erroneous system output.

Similarly, external circumstances should be considered to evaluate the risk normality. It is an inherent risk that an autonomous vehicle might cause a high-velocity collision with an object that suddenly appears, but the same does not hold for an autonomous vacuum robot.

Furthermore, a diligent system user should take precautionary measures to minimise the potential damage the system can cause, as well as the probability that this might occur. The fact that some precautionary measures were not taken does, however, not automatically mean that the system user has not acted diligently. It is only required that he takes reasonable measures. More concretely, system users should ensure that the system achieves a reasonable degree of accuracy.

For a more abstract idea of whether a given degree of accuracy might suffice, data on similar human performance can serve as an important indicator. If the system user can show that his system outperforms the average relevant human being, this serves as an indication of diligence. Consequently, the availability of qualitative data is not only useful to train AI systems, but also to evaluate them. Additionally, if the system user adheres to AI soft law standards, this may serve as another abstract indicator of diligence.

While some unclarity remains unavoidable, due to the limited amount of existing case law and scholarship on the use of AI systems, the elements mentioned above offer some interesting guidelines for AI system users who want to ensure that they do not violate the duty of diligence. This duty will continue to play an important complementary role, even if the European legislator decides to adopt a tort law regime for AI systems. Furthermore, we would argue that our analysis of the application of the duty of diligence to AI system users helps to illustrate that our existing tort and contract law regimes already contain many tools to deal with the use of AI systems in these respective fields. These considerations may prove to be valuable in assessing the need for a specific European tort law regime for AI systems.